

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

COMPUTERS INFECTED WITH EMOTET MALWARE

Case No.

1:21mj567

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ District of _____ Multiple _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1030(a)(5)(A)	Computer Fraud
18 U.S.C. § 371	Conspiracy to Commit Computer Fraud

The application is based on these facts:

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Blair Newman

Applicant's signature

Blair Newman, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
by telephone after e-mailing documents (specify reliable electronic means).

Date:

02/22/21

City and state: Greensboro, North Carolina

L. Patrick Auld

Judge's signature

L. Patrick Auld, United States Magistrate Judge

Printed name and title

ATTACHMENT B
PARTICULAR THINGS TO BE SEIZED

This warrant authorizes the search of the electronic storage media identified in Attachment A and the seizure or copying from the electronic storage media identified in Attachment A electronically stored information that constitutes evidence and/or instrumentalities of the Emotet botnet computer fraud and conspiracy in violation of Title 18, United States Code, Sections 1030(a)(5)(A) (computer fraud) and 371 (conspiracy to commit computer fraud), in that remote access techniques may be used:

1. To search the electronic storage media identified in Attachment A and to seize or copy from the electronic storage media identified in Attachment A any electronically stored information, such as encryption keys and server lists, used by the administrators of the Emotet botnet to communicate with computers that are part of the Emotet botnet infrastructure; and

2. To search the electronic storage media identified in Attachment A and to seize or copy from the electronic storage media identified in Attachment A any electronically stored information, such as IP addresses and routing information, necessary to determine whether any electronic storage media identified in Attachment A continues to be controlled by the

administrators of the Emotet botnet after the seizure or copying of the electronically stored information in Paragraph 1.

This warrant does not authorize the seizure of any tangible property. Except as provided in Paragraphs 1 and 2, this warrant does not authorize the seizure or copying of any content from the electronic storage media identified in Attachment A or the alteration of the functionality of the electronic storage media identified in Attachment A.

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN RE APPLICATION FOR A
WARRANT TO SEARCH
COMPUTERS INFECTED WITH
EMOTET MALWARE

Case No. 1:21mj567

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41(b)(6)(B) FOR A SEARCH WARRANT**

I, Blair Newman, a Special Agent with the Federal Bureau of Investigation (“FBI”), being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. FBI is investigating the Emotet malicious software (“malware”) and its associated botnet. Given its worldwide impact, FBI is collaborating with foreign law enforcement agencies, which have gained access to Emotet-linked servers that are physically located in their respective jurisdictions. A foreign law enforcement agency¹ has replaced a file on one of these servers, located overseas, with a law enforcement-created file. The file has been and will be downloaded by victim computers (i.e., “bots”) throughout the world, including thousands of active victim computers that appear to be located in the United States, during the normal operation of Emotet. In order to receive the

¹ This foreign law enforcement agency is viewed as trustworthy and reliable, based on the experience of the FBI.

file, a victim computer must be powered on and attempt to communicate with the Emotet server on which law enforcement has replaced the file. The law enforcement file provides victim computers with new instructions that untether them from the Emotet botnet and prevent the botnet administrators from communicating with infected computers; it does so by changing the malware's encryption keys and replacing a list of servers controlled by the botnet's administrators with a list of servers controlled by foreign law enforcement.

2. Law enforcement previously obtained three warrants related to this operation, 21MJ29, 21MJ35, and 21MJ47 (hereinafter the "prior warrants"). They authorized the seizure or copying of electronically stored information that constitutes evidence and/or instrumentalities of the Emotet botnet computer fraud and conspiracy from identified computers infected with the Emotet malware that are located in the United States. The most recent authorization, under warrant 21MJ47, expired on February 19, 2021.

3. From on or about January 26, 2021, through February 19, 2021, approximately 2,000 computers located in the United States have received the law enforcement file, as authorized by the prior warrants. However, thousands of computers in the United States known to have been in an active state of Emotet malware infection between April 1, 2020, and January 22, 2021, have yet not received the law enforcement file.

4. Therefore, I make this affidavit in support of an application for a warrant under Federal Rule of Criminal Procedure 41(b)(6)(B) to use remote access techniques to search infected computers that are located in the United States, further identified in Attachment A, and to seize or copy electronically stored information that constitutes evidence and/or instrumentalities of the Emotet malware and botnet, further described in Attachment B.

5. This warrant does not authorize the collection of content of communications from the infected computers, nor does it authorize law enforcement officers to alter the infected computers' operating systems, files, or software, except as expressly provided in this affidavit.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other witnesses and agents, including foreign law enforcement officers. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030(a)(5)(A) (computer fraud) and 371 (conspiracy to commit computer fraud) have been committed in the Middle District of North Carolina and elsewhere.

AGENT BACKGROUND

8. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since May 2019. I am currently assigned to the Cyber Squad in the Raleigh Resident Agency of the Charlotte Division. Previously, from May 2016 to May 2019, I was an FBI Staff Operations Specialist assigned to a Cyber Squad in the New York Office. I have participated in investigations of criminal offenses involving computer and wire fraud, as well as conspiracy, and I am familiar with the means and methods used to commit such offenses. I am an “investigative or law enforcement officer” within the meaning of 18 U.S.C. § 2510; that is, an officer of the United States of America who is empowered to investigate and make arrests for offenses alleged in this warrant.

STATUTORY AUTHORITY

9. Federal Rule of Criminal Procedure 41(b)(6)(B) provides that “a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.”

10. Title 18, United States Code, Section 1030(a)(5)(A) provides that whoever “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . shall be punished as provided in subsection (c) of this section.” Section 1030(e)(2)(B) defines a “protected computer” as a computer “which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]” Section 1030(e)(8) defines “damage” as “any impairment to the integrity or availability of data, a program, a system, or information[.]”

11. Title 18, United States Code, Section 371 provides: “If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.”

PROBABLE CAUSE

A. Overview of the Emotet Malware and Botnet

12. Emotet is a family of malware that targets critical industries worldwide, including banking, e-commerce, healthcare, academia,

government, and technology. Emotet malware primarily infects victim computers through spam email messages containing malicious attachments or hyperlinks. Once it has infected a victim computer, Emotet can deliver additional malware to the infected computer, such as ransomware or malware that steals financial credentials. The computers infected with Emotet malware are part of a botnet (i.e., a network of compromised computers), meaning the perpetrators can remotely control all of the infected computers in a coordinated manner. The owners and operators of the victim computers are typically unaware of the infection.

13. For example, in 2017, the computer network of a school district in the Middle District of North Carolina was infected with the Emotet malware. The Emotet infection caused damage to the school's computers, including but not limited to the school's network, which was disabled for approximately two weeks. In addition, the infection caused more than \$1.4 million in losses, including but not limited to the cost of virus mitigation services and replacement computers. From 2017 to the present, there have been numerous other victims throughout North Carolina and the United States, to include computer networks of local, state, tribal, and federal governmental units, corporations, and networks related to critical infrastructure.

14. Administrators of the Emotet botnet use a system of tiered servers, described here as Tier 1, Tier 2, and Tier 3, to communicate with the Emotet

malware installed on infected computers. Tier 1 servers are typically compromised web servers belonging to what appear to be unknowing third parties. Tier 2 and Tier 3 servers are rented and controlled by the perpetrators. The primary function of the Tier 1 and Tier 2 servers is to forward communications containing encrypted data between infected computers and Tier 3 servers.

15. Emotet malware installed on infected computers contains a list of dozens of Tier 1 servers identified by Internet Protocol (“IP”) address. At regular intervals, roughly every fifteen minutes, the Emotet malware directs victim computers to attempt to communicate with each Tier 1 server in turn (i.e., “beaconing”). After establishing a communication channel, the malware uses the victim computer to send and receive communications to the tiered servers. The Tier 3 servers host control panels used by the perpetrators to send instructions to infected computers; for example, to download an updated version of the Emotet malware or another type of malware, such as ransomware. Data sent in those communications is encrypted using a key known to the perpetrators.

B. Remote Access, Searches, and Seizures

16. Foreign law enforcement agents, working in coordination with the FBI, have gained lawful access to some of Emotet’s Tier 2 and Tier 3 servers physically located in their respective jurisdictions. Through such access,

foreign law enforcement agents² identified the IP addresses of approximately 1.6 million computers worldwide that appear to have been infected with Emotet malware between April 1, 2020 and January 22, 2021, meaning those computers were in a state of infection, not necessarily that the initial infection occurred during that time period. Of those, over 45,000 infected computers appear to be both currently-infected and located in the United States, according to publicly available Whois records and IP address geolocation

17. These computers have been identified as infected with the Emotet malware because they communicated through the Internet with servers that are part of the Emotet botnet infrastructure during the relevant time period. The Emotet malware, as described above, contains a list of dozens of IP addresses of Tier 1 servers, as well as the keys to encrypt communications with those servers. Only infected computers, therefore, are capable of successfully communicating with the Emotet Tier 2 and Tier 3 servers that foreign law enforcement agents have accessed.

18. Infected computers located in the United States constitute “protected computers” within the meaning of Rule 41(b)(6)(B) and § 1030(e)(2)(B) because they are used in or affecting interstate or foreign commerce or communication, based on their connection to the Internet. The

² This information provided by foreign law enforcement agents is reliable, based on the experience of the FBI.

infected computers have been “damaged” within the meaning of Rule 41(b)(6)(B) and § 1030(e)(8) because the Emotet malware has impaired the integrity and availability of data, programs, systems, and information on the infected computers.

19. The thousands of presumptively U.S.-based infected computers appear to be located in five or more judicial districts, according to publicly available Whois records and IP address geolocation. These districts include, but are not limited to, the following: Southern District of Florida; District of Massachusetts; District of New Jersey; Eastern District of New York; Southern District of Ohio; District of Rhode Island; District of South Dakota; and District of South Carolina.

20. Leveraging their access to Tier 2 and Tier 3 servers, agents from a trusted foreign law enforcement partner, with whom the FBI is collaborating, have replaced Emotet malware on servers physically located in their jurisdiction with a file created by law enforcement (hereinafter the “law enforcement file”). This warrant would reauthorize this action for the next two weeks, with the intent that computers in the United States that are infected by the Emotet malware, and have not yet received the law enforcement file, will download the file via Tier 2 and Tier 3 servers during an already-programmed Emotet update.

21. The law enforcement file will prevent the administrators of the Emotet botnet from communicating with infected computers by changing the malware's encryption keys and replacing a list of servers controlled by the perpetrators with a list of servers controlled by law enforcement. This warrant therefore authorizes law enforcement officers to seize or copy from the infected computers any electronically stored information, including the encryption keys and server lists, used by the administrators of the Emotet botnet to communicate with computers that are part of the Emotet botnet infrastructure.

22. Infected computers that have downloaded the law enforcement file will then attempt to establish communication with servers controlled by the trusted law enforcement partner, rather than Emotet Tier 1 servers. In addition, data sent in those communications will be encrypted using a key known to law enforcement. This warrant therefore authorizes law enforcement officers to seize or copy from the infected computers any electronically stored information, including IP addresses and routing information, necessary to determine whether the infected computer continues to be controlled by the administrators of the Emotet botnet.

23. The law enforcement-controlled servers that will replace the Emotet Tier 1 servers will serve as a dead end; that is, they will not further route communications from infected computers. The servers will not capture

content from the infected computers. They will, however, record the IP address and associated routing information of the infected computers for victim notification purposes. U.S. authorities will seek separate pen-trap orders, pursuant to 18 U.S.C. §§ 3121–3127, to the extent any of the law enforcement servers are operated within the United States.

24. The law enforcement file does not collect content from the infected computers, nor does it alter the functionality of the infected computers' operating systems, files, or software, except as expressly provided in this affidavit. The law enforcement file does not remediate malware that was already installed on the infected computer through Emotet, such as ransomware or malware that steals financial credentials; however, it is designed to prevent additional malware from being installed on the infected computer by untethering the victim computer from the botnet.

25. As noted above, foreign law enforcement agents, not FBI agents, have replaced the Emotet malware, which is stored on a server located overseas, with the file created by law enforcement. I seek this warrant out of an abundance of caution, however, in the event U.S. authorities and foreign law enforcement agents may potentially be deemed to be working as part of a joint venture.

TIME AND MANNER OF EXECUTION


26. I request, pursuant to Rule 41(e)(2), that the Court authorize the distribution of the law enforcement file to computers infected with Emotet malware in the United States for a period of fourteen days, beginning on or about February 22, 2021.

27. Because infected computers may attempt to communicate with servers that are part of the Emotet botnet infrastructure at any time, good cause exists to permit the execution of the requested warrant at any time in the day or night.

CONCLUSION

28. I submit that this affidavit supports probable cause for a warrant to use remote access to search electronic storage media described in Attachment A and to seize or copy electronically stored information described in Attachment B.


Respectfully submitted,



Blair Newman
Special Agent
Federal Bureau of Investigation

Dated: February 22, 2021

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of this written affidavit.



L. Patrick Auld
United States Magistrate Judge
Middle District of North Carolina